REMARKS

Claims 1-17, 21 and 22 were previously pending. Claims 1-6, 8, 11 and 17 are amended. Claims 21 and 22 are canceled. No claims are added. Claims 1-17 remain pending.

Examiner Interview

Applicant thanks the Examiner for the personal interview on May 17, 2006 wherein the application was discussed in general but the claims were not specifically discussed. The specification has been amended to reflect one aspect of the discussion. It was also discussed that the O'Shea reference was indeed published in April 2001 and therefore is not prior art for the present application, filed November 13, 2001, less than one year after said publication.

35 U.S.C. § 112 Rejections

Claims 1-17, 21 and 22 stand rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Applicant respectfully traverses the rejection as it remains relevant.

Regarding **claims 1, 2, 3, 5, 6, 8, 11, 17 and 21**, the language objected to by the Examiner ("usable to route a message to the first computing device....") has been removed, thus rendering the rejection moot as to these claims.

Regarding **claims 3, 4 and 5**, the language objected to by the Examiner ("then the public key is discarded) has been removed, thus rendering the rejection moot as to these claims.

Claim 14 recites "if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then discarding the public key and first network address without caching them."

Claim 15 recites "if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache."

Applicant contends that the specification, in paragraph [0044], supports the language of claims 14 and 15 where it reads:

> If no duplicate association was found in step 814, then step 818 looks for a match of just the network address. If one is found, there may be a problem: two public keys (the one already in the cache and the one in the present message) have been found to be associated with the same network address. This may indicate a brute force attack in which an attacker generates public keys until it finds one that, through the procedures of FIGS. 3 and 4 and the accompanying text, produces a network address to match the one produced by a legitimate sender. The safe course for the recipient is to consider the network address compromised. **The message is discarded** and **the association in the cache with the matching network address is also discarded** in step 820. (Emphasis added).

Claim 16 recites "if the timer expires, removing the public key/network address association from the cache." Relevant to this element, the specification states in paragraph [0044]: "In some embodiments, each association in the cache is discarded after a period of non-use. In these embodiments, step 816 resets the use timer of the association already in the cache that matches the values in the present message." Applicant contends that this language from the specification adequately supports the language recited in claim 16.

Accordingly, the Section 112 rejections should be withdrawn.

35 U.S.C. § 103 Rejections

Claims 1-17, 21 and 22 stand rejected under 35 U.S.C. 103(a) as being anticipated by U.S. Patent No. Re. 36,946 to Diffie, et al. (hereinafter "Diffie") in view of Greg O'Shea, "Child-proof Authentication for MIPv6 (CAM)", (ACM SIGCOMM Computer Communication Review, Vol. 31, Issue 2, April 2001). Applicant respectfully traverses the rejection.

Applicant originally and mistakenly identified O'Shea as being published in 2000 but has since shown that the actual publication date was April, 2001. As such, O'Shea was not published more than one year prior to the filing date (November 13, 2001) of the present application. Therefore, O'Shea is not prior art for the present application.

That leaves Diffie standing alone to disclose, teach or suggest each and every element in each of the rejected claims.

Claim 1 has been amended and now recites a "method for a first computing device to make authentication information available to a second computing device. The method comprises steps of "creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device derived from ***a portion*** **of a hash of the public key**, and a digital signature, the digital signature generated by hashing the network address and at least a portion of the content data with a private key corresponding to the public key of the first computing device. A step of "making the authentication information available to the second computing device" is also recited in claim 1.

The emphasized portions of claim 1 stress that the first (sending) computing device derives its network address by hashing a public key of the first computing device and using a portion of the result as a part of the network address. This feature is not disclosed, taught or suggested by Diffie.

Accordingly, claim 1 is allowable over the cited references and the rejection of claim 1 should be withdrawn.

Claim 2 recites a computer-readable medium including instructions that, when executed, perform steps of a method similar to the method recited in claim 1. The amendment to claim 2 further defines deriving a portion of a network address from a public key to be deriving a portion of the address from "a portion of a hash of the public key."

This element of claim 2 is not taught or suggested by the cited art and, therefore, claim 2 is allowable and the rejection thereof should be withdrawn.

Claim 3 recites a method for a receiving (second) computing device to authenticate content data made available by a sending (first) computing device. The method includes steps of: "accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature."

The receiving computing device generates a value (a "second network address") from the public key by hashing the public key. If a portion of the result of this hash matches a portion of the (first) network address sent from the first computing device, the content is accepted if the digital signature is also found to be valid.

This element of claim 3 is not taught or suggested by the cited reference and is thus allowable over the cited art. Accordingly, the rejection of claim 3 should be withdrawn.

Claim 4 depends from claim 3 and is allowable at least by virtue of that dependency. Accordingly, the rejection of claim 4 should be withdrawn.

Claim 5 has been amended and now recites a computer-readable medium storing instruction for performing a method for a receiving device to authenticate a content sent from a sending device. The method includes a step of accessing authorization information made available by the sending device. The authentication information includes content data, a public key of the sending device, a network address of the sending device and a digital signature. The network address has a node-selectable portion that was created by taking a portion of a result of hashing the public key.

The method also includes a step of the receiving device hashing the public key received from the sending device and taking a portion thereof to derive a node-selectable portion of a second address.

If the derived node-selectable portion of the second address matches a portion of the node-selectable portion of the first address and the digital signature is valid, the content is accepted.

It is also recited in claim 5 that the public key of the sending device is access over an unsecure channel.

The cited reference does not teach or suggest all of the elements of claim 5. Therefore, claim 5 is allowable over the cited art and the rejection of claim 5 should be withdrawn.

Claim 6 has been amended and now recites a "method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device." The method includes steps of: (1) "hashing the public key;" (2) "comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion;" (3) "if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing;" and (4) "if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing."

Claim 6 is supported by paragraph [0041] (and others) of the specification where a general rule that "the cryptographic strength of an authentication mechanism that uses a hash increases with the number of bits produced by the hash." The language of claim 6 includes the opportunity to utilize a greater number of bits than recited in previous claims.

Most of the specification discusses utilizing a portion of the 62 changeable bits of a node-selectable portion of a network address. It also states that a "u" bit and a "g" bit cannot be changed, thus the 62 bits (a 64-bit word minus the "u" and "g" bits).

Paragraph [0044] discusses how these two bits can also be utilized by hashing the public key and using the hash value if the hash value matches the "u" and "g" bits. If the hash value doesn't match those bits, then a modifier is appended to the public key and a hash value is taken of the composite number.

If that hash value matches the "u" and "g" bits, then that value is used. Otherwise, the process repeats until the hash value matches the unchangeable bits.

The cited reference does not disclose, teach or anticipate this element of claim 6. Accordingly, claim 6 is allowable over the cited references and the rejection thereof should be withdrawn.

Claim 7 depends from claim 6 and is allowable by virtue of that dependency. Claim 7 further identifies the additional bits portion of the network address as being the "u" and "g" bits. Accordingly, claim 7 is allowable over the cited art and the rejection thereof should be withdrawn.

Claim 8 recites a computer-readable storage medium storing instructions for performing a method for "a computing device to derive a node-selectable portion of a network address from a public key of the computing device." The method comprises steps of: "hashing the public key" and "comparing a portion of a value produced by the hashing with a portion of the network address **other than the node-selectable portion.**" If the portions do not match, "choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing" and "if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing."

These elements are similar to those of claim 6 except that instead of expanding the hashed number by only two bits, a greater number of bits is taken from a portion of the address other than the node-selectable portion, i.e. the route prefix of the address. This significantly enhances security of the process.

The cited art does not teach or suggest the elements recited in claim 8. Accordingly, claim 8 is allowable over the cited art and the rejection thereof should be withdrawn.

Claims 9 and 10 also utilize a hashing a portion of the route prefix of the network address as well as the node-selectable portion of the network address. By the same rationale discussed for claim 8, above, these claims are allowable over the cited art and the rejection of these claims should also be withdrawn.

Claim 11 recites a method for a second computing device to maintain a cache of at least one public key/network address association." The method comprises steps of: (1) "accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;" (2) "deriving a portion of a second network address from the public key of the first computing device;" (3) "validating the digital signature by using the public key of the first computing device;" and (4) "caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from at least one of the content data and a hash value of data including the content data."

Claims 12-16 depend from claim 11 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should also be withdrawn.

Claim 17 recites a "method for a second computing device to maintain a cache of at least one public key/network address association." The method includes accessing authentication information made available by a first computing device. This may either be done by receiving a message containing the authentication information or retrieving a portion of the information from some location.

The authentication information includes "content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature." The second device derives "deriving a portion of a second network address from the public key of the first computing device" and validates the digital signature.

The method also includes a step of "caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from at least one of the content data and a hash value of data including the content data."

The cited reference does not teach or suggest these elements. Therefore, claim 17 is allowable over the cited art and the rejection should be withdrawn.

CONCLUSION

In view of the foregoing remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this response, that the application is not in condition for allowance, the Examiner is encouraged to call the Applicant's attorney at the telephone number listed below. If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, please charge any deficiency to **Deposit Account No. 50-0463.**

Respectfully submitted,

MICROSOFT CORPORATION

Date: May 30, 2006

By: James R. Banowsky

James R. Banowsky, Reg. No. 37,773
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399
Telephone (425) 705-3539

CERTIFICATE OF MAILING OR TRANSMISSION
(Under 37 CFR § 1.8(a)) or ELECTRONIC FILING

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

May 30, 2006
Date

Noemi Tovar
Signature

Noemi Tovar
Printed Name